PROCEDE D'AUTHENTIFICATION ANONYME

La présente invention se rapporte à un procédé d'authentification par clé secrète d'au moins un utilisateur, en vue par exemple d'autoriser ou non cet utilisateur à accéder à des ressources lorsque l'anonymat de l'utilisateur qui s'authentifie est requis.
Dans la présente description, le terme de ressources doit être pris avec une acceptation très large et désigne de manière générale toute fonction, application, service, ensemble de données à laquelle un utilisateur peut accéder et dont l'accès est conditionné par une autorisation préalable délivrée à l'issue d'une procédure d'authentification. A titre d'exemple non limitatif, il peut s'agir d'un service fourni par un serveur spécialisé, une fonction d'accès à un réseau, une ressource informatique telle qu'une base de données ou une application logicielle disponible sur un serveur et pouvant être partagée par plusieurs utilisateurs.

D'une manière générale, l'authentification est un service de sécurité réalisé par une entité d'authentification, dont l'objectif est de valider l'identité d'un utilisateur qui souhaite s'identifier, apportant par là même la preuve de la légitimité de cet utilisateur à accéder aux ressources concernées. Une entité d'authentification désigne communément tout équipement, machine ou système informatique qui permet de centraliser un processus d'authentification et qui est accessible par des utilisateurs souhaitant s'authentifier pour l'accès à des ressources, via un réseau de télécommunication.
De façon usuelle, un utilisateur souhaitant déclencher un processus d'authentification dispose d'une entité cliente lui permettant de communiquer avec l'entité

d'authentification. Une entité cliente dans la présente description, désigne tout système ou équipement électronique permettant d'échanger des données avec l'entité d'authentification, de préférence sans contact. Selon l'art antérieur, l'authentification par clé secrète se caractérise essentiellement par la succession d'étapes suivantes telles que représentées à la figure 1. Ainsi, lorsque une entité cliente A souhaite s'authentifier auprès d'une entité d'authentification B, elle fournit dans un premier temps son identité à l'entité B, sous la forme d'un identifiant statique qui lui est spécifique, et la prouve ensuite par l'utilisation d'une clé secrète K_A connue et partagée par les entités A et B seulement. Pour ce faire, lorsque l'entité d'authentification B reçoit une demande d'authentification émise par une entité cliente se présentant à elle comme détentrice de l'identité A, ladite entité d'authentification génère d'abord un nombre aléatoire appelé aléa, ou encore appelé challenge, et envoie cet aléa à l'entité cliente A. En retour, l'entité cliente chiffre, on dit encore signe, l'aléa reçu selon un algorithme cryptographique prédéfini à clé secrète, tel que l'algorithme DES (acronyme anglo-saxon pour « Data Encryption Standard »). L'entité A renvoie alors à l'entité d'authentification B la valeur $C(K_A, \text{aléa})$, où C est une fonction cryptographique. L'entité B effectue de son côté le même calcul en utilisant la fonction cryptographique C et la clé secrète de A K_A, et compare le résultat obtenu avec la valeur que lui a retourné l'entité A. En cas de cohérence entre le résultat attendu et la valeur que lui a retournée A, l'entité d'authentification B valide l'authentification, signifiant ainsi que A a réussi à s'authentifier. La

validation de l'authentification se traduit par exemple par l'envoi par l'entité d'authentification à destination de l'entité cliente A qui a été authentifié, des droits d'accès aux ressources.

De telles méthodes d'authentification à clé secrète sont largement répandues dans les réseaux de télécommunications, mais présentent toutefois un certain nombre d'inconvénients en ce qui concerne la garantie de l'anonymat de l'entité cliente souhaitant s'authentifier. En effet, pour initialiser le processus d'authentification, un identifiant spécifique de l'entité cliente est nécessairement transmis en clair à l'entité d'authentification. Ainsi, un tiers malveillant est à même de connaître l'identifiant spécifique de l'entité qui s'authentifie par l'observation de la transaction entre l'entité d'authentification et l'entité s'authentifiant.

De plus, l'identifiant spécifique d'une entité souhaitant s'authentifier peut également être déduite par un tiers malveillant agissant cette fois de façon active, c'est-à-dire en initialisant un processus d'authentification en se faisant passer pour une entité d'authentification vis-à-vis de l'entité s'authentifiant.

Une entité s'authentifiant peut encore être reconnue par l'observation de son comportement et, plus particulièrement par l'observation des réponses fournies par l'entité au cours de processus d'authentification antérieurs.

En effet, les réponses fournies par une entité s'authentifiant sont caractéristiques de certaines entrées correspondant aux aléas qui lui ont été soumis par l'entité d'authentification et, pour une même entrée, l'entité s'authentifiant fournira toujours la même réponse. En observant au préalable la réponse de l'entité à des valeurs caractéristiques d'aléa, il est possible de reconnaître une entité s'authentifiant en lui soumettant à nouveau une de ces valeurs d'aléa pour laquelle une réponse de l'entité a déjà été observée. Ainsi, une entité qui signe des aléas pour s'authentifier peut être caractérisée par sa réponse pour une valeur d'aléa particulière (par exemple, 0, 10, 100, 1000, etc....). En observant deux identifications successives avec le même aléa, il est donc possible de déduire si ce sont deux entités distinctes ou la même entité qui se sont authentifiées.

La présente invention a pour but de remédier à ces inconvénients en proposant un procédé d'authentification basé sur un algorithme de chiffrement à clé secrète, dans lequel l'anonymat de l'entité s'authentifiant est garanti, de sorte à ce que seule une entité d'authentification légitime puisse reconnaître l'identité de l'entité qui s'authentifie et personne d'autre.

Avec cet objectif en vue, l'invention a pour objet un procédé d'authentification d'au moins une entité cliente par une entité d'authentification, ladite entité d'authentification comprenant un ensemble de clés secrètes, chacune étant associée à une entité cliente susceptible d'être identifiée par ladite entité

d'authentification, ledit procédé étant caractérisé en ce qu'il comprend les étapes suivantes consistant à :

a-transmettre une demande d'authentification anonyme de la part de l'entité cliente vers l'entité d'authentification ;

b-envoyer de l'entité d'authentification vers l'entité cliente, une valeur de compteur d'authentification correspondant à l'état courant d'un compteur de l'entité d'authentification;

c-vérifier, côté entité cliente, que la valeur de compteur d'authentification reçue est strictement supérieure à une valeur de compteur mémorisée par l'entité cliente ;

d-calculer, côté entité cliente, une signature de compteur par application d'une fonction cryptographique partagée par l'entité cliente et l'entité d'authentification, avec comme opérandes ladite valeur de compteur d'authentification et une clé secrète associée à l'entité cliente ;

e-transmettre ladite signature de compteur à l'entité d'authentification ;

f-mettre à jour la valeur de compteur mémorisée par l'entité cliente avec ladite valeur de compteur d'authentification;

g-rechercher, côté entité d'authentification, au moins une entité cliente susceptible d'être identifiée, pour laquelle la signature de compteur correspondante pour ladite valeur de compteur d'authentification est cohérente avec la signature de compteur reçue ;

h-faire croître le compteur d'authentification.

De préférence, les étapes b) à h) sont réitérées au moins une fois, de sorte à s'assurer que l'entité cliente identifiée est identique à chaque itération.

Selon un mode de réalisation particulier, l'étape de recherche consiste à :

i-calculer, pour chaque entité cliente susceptible d'être identifiée, la signature de compteur correspondante par application de la fonction cryptographique avec comme opérandes la valeur de compteur d'authentification et la clé secrète associée, de sorte à établir une liste de couples entité cliente susceptible d'être identifiée/signature de compteur correspondante, pour ladite valeur de compteur;

j-vérifier la cohérence entre la signature de compteur reçue et au moins une signature de compteur de ladite liste.

De préférence, la liste des couples entité cliente susceptible d'être identifiée/signature de compteur correspondante établie pour une valeur de compteur d'authentification donnée, est ordonnée, côté entité d'authentification, selon la valeur de ladite signature de compteur.

Selon ce mode de réalisation, en cas de cohérence entre la signature de compteur reçue et la signature de compteur d'une pluralité de couples, les étapes b) à h) sont réitérées jusqu'à obtention d'un couple unique pour lequel la signature de compteur correspond à la signature de compteur reçue.

De préférence, lors de la répétition de l'étape i), la signature de compteur est calculée uniquement pour les entités clientes correspondant à ladite pluralité de couples déterminée à l'itération précédente.

Dans une variante, le procédé selon l'invention consiste à mettre en œuvre l'étape i) de manière anticipée par rapport à une demande d'authentification issue d'une entité cliente à l'étape a), ladite étape i) anticipée consistant à pré-établir, côté entité d'authentification, pour au moins une valeur de compteur d'authentification à venir, la liste des couples entité cliente susceptible d'être identifiée/signature de compteur correspondante pour chacune desdites valeurs de compteur d'authentification à venir, et à mémoriser lesdites listes pré-établies côté entité d'authentification, tout envoi de l'entité d'authentification vers l'entité cliente d'une valeur de compteur d'authentification, correspondant à l'envoi d'une valeur de compteur d'authentification pour laquelle une liste des couples entité cliente susceptible d'être identifiée/signature de compteur correspondante a déjà été pré-établie.

De préférence, l'étape h) consiste à faire croître le compteur d'authentification d'un pas fixe.

Dans une variante, l'étape h) consiste à faire croître le compteur d'authentification d'un pas aléatoire.

Selon un mode de réalisation particulier, en réponse à une demande d'authentification, l'étape b) consiste à envoyer, côté entité d'authentification, en plus de la valeur de compteur d'authentification, une valeur aléatoire associée à ladite valeur de compteur, ladite valeur aléatoire étant différente pour chacune des valeurs de compteur d'authentification envoyée, chaque étape de signature de compteur mise en œuvre au cours dudit procédé étant remplacée par une étape de signature du couple valeur de compteur d'authentification/valeur

aléatoire associée, consistant en l'application de la fonction cryptographique comprenant en plus comme opérande ladite valeur aléatoire associée.

Selon une variante, l'étape c) consiste en outre à vérifier que la différence entre la valeur de compteur d'authentification reçue et la valeur de compteur mémorisée par l'entité cliente est inférieure ou égale à une valeur prédéterminée.

Dans une variante, lorsque l'étape c) n'est pas vérifiée, les étapes intermédiaires suivantes sont mises en œuvre consistant à :

-envoyer de l'entité cliente vers l'entité d'authentification, la valeur de compteur mémorisée par l'entité cliente ;

-envoyer de l'entité d'authentification vers l'entité cliente, une valeur de compteur d'authentification temporaire supérieure à ladite valeur de compteur mémorisée par l'entité cliente, puis à :

-mettre en oeuvre les étapes d) à g) sur la base de la valeur de compteur d'authentification temporaire et, en cas de succès de l'authentification de ladite entité cliente,

-mettre à jour la valeur de compteur d'authentification correspondant à l'état courant du compteur de l'entité d'authentification avec la valeur de compteur d'authentification temporaire et mettre en œuvre l'étape h).

De préférence, l'étape e) consiste à transmettre en outre à l'entité d'authentification la valeur de compteur d'authentification.

De préférence, la valeur de compteur d'authentification est codée sur au moins 128 bits.
L'invention concerne également une carte à puce, caractérisé en ce qu'elle comprend un circuit intégré et des moyens de mémorisation d'une clé secrète et de mise en œuvre du procédé selon l'invention.
De préférence, il s'agit d'une carte à puce sans contact.
L'invention concerne encore une entité d'authentification d'au moins une entité cliente, caractérisé en ce qu'elle comprend un lecteur de carte à puce doté de moyens pour la mise en œuvre du procédé selon l'invention.
De préférence, l'entité d'authentification comprend un lecteur de carte à puce sans contact.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante donnée à titre d'exemple illustratif et non limitatif et faite en référence aux figures annexées dans lesquelles :

-la figure 1 est un schéma illustrant un processus d'authentification par clé secrète selon l'état de la technique, et a déjà été décrite ;

-la figure 2 est un schéma illustrant les principales étapes du procédé d'authentification selon la présente invention.

La figure 2 décrit donc les étapes principales du procédé d'authentification par clé secrète d'une entité cliente A par une entité d'authentification B, selon la présente invention.

L'entité A souhaitant s'authentifier possède une clé secrète K_A qui lui est propre, un moyen de mémorisation d'une valeur de compteur CA, ainsi qu'une fonction cryptographique de signature S, partagée également par l'entité d'authentification B, et qui est prévue pour s'appliquer avec les deux opérandes suivants : une clé secrète et une valeur de compteur, de sorte à signer la valeur de compteur.

L'entité d'authentification B comprend quant à elle une liste de couples (Ai, K_{Ai}), Ai étant le nom d'une des n entités clientes susceptibles d'être authentifiées par l'entité d'authentification B et K_{Ai} étant la clé secrète associée à l'entité cliente Ai qui lui est propre. L'entité d'authentification B comprend également un compteur COMPTB délivrant une valeur de compteur CB et la fonction cryptographique S, identique à celle implémentée dans l'entité cliente A.

Le déroulement du processus d'authentification anonyme selon l'invention est le suivant. Dans une première étape, lorsque l'entité cliente A veut s'authentifier auprès de l'entité d'authentification B, elle se signale à B par la transmission d'une demande d'authentification anonyme « DemandeAuthentification ». En réponse, dans une deuxième étape, l'entité d'authentification B envoie vers l'entité cliente A la valeur de compteur CB correspondant à l'état courant de son compteur COMPTB.

Dans une troisième étape, l'entité cliente A compare la valeur de compteur CB reçue avec la valeur de compteur CA

mémorisée par l'entité cliente A. A ce stade, deux possibilités s'offrent à l'entité cliente A :

Soit CA ≥ CB, alors l'entité cliente A ne fait plus rien car cette situation signifie qu'une entité essaye de faire rejouer une signature à l'entité cliente A. Or, selon une caractéristique de l'invention, pour ne pas être reconnaissable par son comportement, une entité cliente ne signe jamais deux fois les mêmes données. Cette situation met donc fin au processus d'authentification.

Soit CA < CB, alors l'entité cliente A peut avoir confiance en l'entité d'authentification B car la valeur de compteur reçue CB étant supérieure strictement à la valeur de compteur mémorisée par A, cela signifie que cette valeur de compteur CB ne lui a encore jamais été soumise pour signature. Le processus passe alors à l'étape suivante.

Dans une quatrième étape, l'entité cliente A signe la valeur de compteur reçue CB par application de la fonction cryptographique S avec comme opérandes la clé secrète K_A associée à l'entité cliente A et la valeur de compteur CB. Le résultat de cette opération de signature de compteur $S(K_A, CB)$ est transmis de l'entité cliente A vers l'entité d'authentification B. L'entité cliente A met alors à jour dans une cinquième étape sa valeur de compteur mémorisée CA avec la dernière valeur de compteur licite qui lui a été transmis par l'entité d'authentification B, à savoir CB.

Dans une sixième étape, l'entité d'authentification B recherche au moins une entité cliente Ai parmi les n entités clientes qu'elle est capable d'authentifier, pour laquelle la signature correspondante de la valeur de compteur CB $S(K_{Ai}, CB)$ est cohérente avec la signature de compteur reçue de l'entité cliente qui cherche à s'authentifier $S(K_A, CB)$.

Si aucune entité cliente susceptible d'être identifiée n'est trouvée, alors cela signifie que l'authentification a échoué. A l'inverse, si exactement une entité cliente Ai est trouvée à l'issue de la phase de recherche pour laquelle $S(K_{Ai}, CB) = S(K_A, CB)$, alors l'entité d'authentification B en conclut que A = Ai. Cela signifie que c'est l'entité cliente Ai qui a cherché à s'authentifier auprès de l'entité d'authentification B et que cette authentification a réussi.

Dans une septième et dernière étape mettant fin au processus d'authentification, l'entité d'authentification B fait croître la valeur de compteur CB pour une prochaine demande d'authentification.

Il est possible qu'un fraudeur, en renvoyant un nombre tiré au hasard, tombe sur une valeur $S(K_{Ai}, CB)$ qui existe et donc se fasse passer pour l'entité cliente Ai. Pour éviter ce risque, l'entité d'authentification B peut systématiquement faire refaire le processus d'authentification au moins une seconde fois de sorte à s'assurer qu'il reconnaît chaque fois la même entité cliente. Le processus peut même être répétée N fois, jusqu'à obtenir une probabilité de tomber au hasard N

fois sur une valeur de signature correspondant à la même entité cliente suffisamment faible.

Egalement, une autre optimisation du processus d'authentification concerne la gestion des cas de collision. En effet, à l'issue de la sixième étape, on peut aboutir à un cas de collision, c'est-à-dire que plusieurs entités clientes Ai susceptibles d'être identifiées par l'entité d'authentification B ont été trouvées pour lesquelles la signature de compteur $S(K_{Ai}, CB)$ est cohérente avec la signature de compteur reçue $S(K_A, CB)$. Il existe en effet une probabilité faible, mais non nulle, pour la fonction cryptographique de signature S fournisse un résultat identique pour deux données différentes. Dans cette situation de collision, il est nécessaire de répéter les étapes du procédé à partir de la deuxième étape, avec une valeur de compteur CB incrémentée à chaque répétition, jusqu'à l'obtention d'une entité cliente Ai susceptible d'être identifiée unique, pour laquelle $S(K_{Ai}, CB) = S(K_A, CB)$.

La sixième étape, consistant en la phase de recherche par l'entité d'authentification d'au moins une entité cliente Ai parmi les n entités clientes qu'elle est capable d'authentifier, pour laquelle la signature correspondante de la valeur de compteur CB $S(K_{Ai}, CB)$ est cohérente avec la signature de compteur reçue de l'entité cliente qui cherche à s'authentifier $S(K_A, CB)$, peut être mise en œuvre de la manière suivante. L'entité d'authentification B calcule, pour chaque entité cliente Ai susceptible d'être identifiée, la signature de compteur correspondante $S(K_{Ai}, CB)$ par application de la fonction

cryptographique S avec comme opérandes la valeur de compteur d'authentification CB et la clé secrète associée K_{Ai}, de sorte à établir une liste de couples entité cliente susceptible d'être identifiée/signature de compteur correspondante (Ai, $S(K_{Ai}, CB)$), pour la valeur de compteur CB courante.

Une fois cette liste établie, l'entité d'authentification la parcourt pour vérifier s'il existe au moins une entité cliente susceptible d'être identifiée Ai vérifiant $S(K_{Ai}, CB) = S(K_A, CB)$.

Dans le cas où plusieurs couples (Ai, $S(K_{Ai}, CB)$) correspondent, on a vu qu'il était nécessaire de répéter les opérations d'envoi et de signature d'une valeur de compteur CB. Néanmoins, cette répétition peut encore aboutir à l'existence de plusieurs couples (Ai, $S(K_{Ai}, CB)$) qui correspondent. Dans ce cas, il est prévu de ne chercher les couples possibles que parmi les couples ayant déjà été sélectionnés aux itérations précédentes. Ainsi, le procédé convergera plus vite vers une entité cliente Ai unique puisque, à chaque itération, la signature de compteur $S(K_{Ai}, CB)$ est calculée uniquement pour les entités clientes Ai correspondant aux couples (Ai, $S(K_{Ai}, CB)$) sélectionnée à l'itération précédente.

A la sixième étape, la phase de calcul par B, pour chaque entité cliente Ai susceptible d'être identifiée, de la signature de compteur correspondante $S(K_{Ai}, CB)$, de sorte à établir la liste de couples entité cliente susceptible d'être identifiée/signature de compteur correspondante (Ai, $S(K_{Ai}, CB)$), pour la valeur de compteur CB courante

peut être très longue et pénalisante en termes de temps de réponse. Pour régler ce problème, selon une variante de l'invention, il est prévu que l'entité d'authentification B pré-calcule, pour au moins une valeur de compteur d'authentification CB à venir, les listes de couples (Ai, $S(K_{Ai}, CB)$) pour ces valeurs CB à venir et mémorise ces résultats. Ainsi, lorsqu'une entité cliente souhaitera s'authentifier par l'envoi du message DemandeAuthentification, l'entité d'authentification B répondra en envoyant une valeur de compter d'authentification CB pour laquelle la liste (Ai, $S(K_{Ai}$, CB)) aura déjà été établie. De manière générale, selon ce mode de réalisation, tout envoi de B vers A d'une valeur de compteur d'authentification CB correspondra à une valeur de compteur d'authentification pour laquelle une liste (Ai, $S(K_{Ai}, CB)$) aura déjà été établie.

La phase de vérification par l'entité d'authentification B, consistant à rechercher l'existence d'au moins une entité cliente Ai de la liste (Ai, $S(K_{Ai}$, CB)) pour laquelle $S(K_{Ai}, CB) = S(K_A, CB)$ peut également être très longue en cas de recherche séquentielle, en théorie de l'ordre de n/2 tests avec une liste comportant n éléments. Aussi, pour optimiser cette phase, la liste des couples obtenus (Ai, $S(K_{Ai}, CB)$) peut être ordonnée de façon croissante (ou décroissante) selon la valeur de la signature de compteur $S(K_{Ai}, CB)$. La recherche d'un couple dans cette liste ordonnée pour lequel la signature de compteur $S(K_{Ai}, CB)$ correspond à $S(K_A, CB)$ peut alors être faite selon une recherche dichotomique. L'entité cliente recherchée est dans ce cas trouvée en moyenne

après avoir effectué $\log_2$ (n) opérations, ce qui procure un gain de temps important.

Le compteur CB étant unique pour chaque authentification, il peut être utilisé comme identifiant de session d'authentification. Ainsi, si plusieurs entités Ai sont en train de se faire authentifier simultanément par l'entité B, cette dernière peut distinguer les dialogues grâce à cette valeur. Il suffit pour cela que les entités clientes cherchant à s'authentifier retournent la valeur CB en plus de la valeur de signature S (KA, CB).

De préférence, le compteur COMPTB fournissant la valeur de compteur d'authentification CB croît d'un pas fixe. Toutefois, le fait que le compteur CB croisse d'un pas fixe permet de prévoir les valeurs de compteur d'authentification qui seront utilisées lors des authentifications à venir. De ce fait, un pirate peut demander plusieurs valeurs $S(K_A, CB)$ à une entité A pour plusieurs valeurs de compteurs CB et, ultérieurement, chercher à s'authentifier auprès de l'entité B en lui retournant les valeurs précédemment obtenues de l'entité cliente A. Ainsi, le pirate peut s'authentifier en se faisant passer pour A. Deux types de parade contre une telle attaque au système d'authentification peuvent être mises en œuvre.

Tout d'abord, une première parade consiste à faire croître le compteur COMPTB d'un pas aléatoire à chaque authentification, de sorte à ne plus utiliser des valeurs successives de CB. Dans ce cas, le compteur devra avoir une capacité plus grande afin de ne pas venir en butée.

Une autre parade consiste à ne plus faire signer à l'entité cliente A cherchant à s'authentifier une simple valeur de compteur CB, mais un couple (CB, aléa), CB s'incrémentant régulièrement et aléa prenant des valeurs aléatoires. La valeur aléatoire est prévue pour être différente pour chacune des valeurs de compteur d'authentification envoyée, et chaque étape de signature de compteur mise en œuvre au cours du procédé d'authentification dans l'une quelconque de ses variantes est alors remplacée par une étape de signature du couple (CB, aléa), consistant en l'application de la fonction cryptographique S avec en plus comme opérande ladite valeur aléatoire associée.

Le procédé d'authentification tel qu'il vient d'être décrit est vulnérable aux attaques par saut de compteur, basées sur le fait que les entités A et B se synchronisent sur la valeur de compteur CB à chaque authentification. Ainsi, une machine malveillante peut se faire passer pour l'entité d'authentification B et envoyer à l'entité cliente A cherchant à s'authentifier une valeur de compteur beaucoup plus grande que la valeur de compteur d'authentification CB effective, correspondant à la valeur courante du compteur COMPTB de l'entité B. En mettant à jour sa valeur de compteur mémorisée CA avec cette grande valeur qui lui est soumise, l'entité A ne pourra plus répondre suite à une demande d'authentification tant que la valeur de compteur CB de l'entité d'authentification B n'aura pas rattrapée cette valeur CA, à cause du test de la troisième étape. De plus, si la machine malveillante fournit à l'entité A

une valeur de compteur maximale, cette dernière, en mettant à jour sa valeur de compteur mémorisée CA à cette valeur maximale, devient définitivement inutilisable par la suite.

Les parades à ces attaques portent plus particulièrement sur la troisième étape du procédé d'authentification, où l'entité cliente A compare la valeur de compteur CB reçue avec la valeur de compteur CA mémorisée par l'entité cliente A.

Dans le cas où CA ≥ CB, selon une variante de l'invention, les étapes intermédiaires suivantes sont mises en œuvre :
-l'entité A signale à l'entité B que sa valeur de compteur mémorisée CA est plus grande que la valeur CB et lui renvoie CA ;

-l'entité B envoie à A une valeur de compteur $CB_{temporaire}$ > CA ;

puis, les autres étapes du procédé d'authentification sont mises en œuvre sur la base de cette valeur de $CB_{temporaire}$ et, si l'authentification de l'entité A réussit avec $CB_{temporaire}$, alors l'entité B met à jour sa valeur de compteur d'authentification CB correspondant à l'état courant de son compteur COMPTB avec la valeur de compteur d'authentification $CB_{temporaire}$. Enfin, le compteur est incrémenté pour une prochaine authentification. Ce processus permet à l'entité d'authentification de se prémunir contre une attaque par saut de compteur. En effet, elle va d'abord authentifier l'entité cliente A

avec $CB_{temporaire}$, avant de mettre à jour son compteur. Ce processus permet également à l'entité cliente A de synchroniser le compteur de l'entité d'authentification B avec sa valeur de compteur mémorisée, si ce dernier avait subi une attaque par saut de compteur.

A ce stade, l'entité B peut aussi implémenter des protections supplémentaires. Par exemple, B peut n'autoriser qu'un certain nombre de ces synchronisations de compteur par entité cliente et par période. Egalement, B peut n'autoriser ces protections que dans une limite raisonnable où la différence entre la valeur de compteur mémorisée par l'entité cliente CA et la valeur de compteur d'authentification CB est inférieure à une valeur prédéterminée.

Selon une autre variante, à la troisième étape du procédé, dans le cas où la relation $CA < CB$ est vérifiée, on vérifie en outre, côté entité cliente, que la différence entre la valeur de compteur d'authentification CB reçue et la valeur de compteur CA mémorisée par l'entité cliente est inférieure ou égale à une valeur prédéterminée Δ, soit $CB - CA \leq \Delta$. L'entité A n'accepte de signer la valeur de compteur CB que si cette condition supplémentaire est vérifiée. Cette condition supplémentaire permet à l'entité cliente A cherchant à s'authentifier de limiter les attaques par saut de compteur en n'acceptant qu'une incrémentation modérée de sa valeur de compteur mémorisée et en ignorant les sollicitations utilisant une valeur de compteur d'authentification très supérieure à sa valeur de compteur mémorisée.

Selon un exemple de réalisation, les valeurs de compteur CA et CB peuvent être des nombres binaires codés sur au moins 128 bits, ce qui permet d'exécuter 2^{128} authentifications avant que le système n'arrive à l'exhaustion du compteur COMPTB.

Les étapes du procédé selon l'invention côté entité cliente, sont par exemple implémentées sur une carte à puce, de préférence une carte à puce sans contact. Une carte à puce pour la mise en œuvre des étapes du procédé selon l'invention ne nécessite que peu de capacité de calcul dans la mesure où les opérations à exécuter sont simples (au plus la signature d'un compteur). L'entité d'authentification se présente alors sous la forme d'un lecteur de carte à puce avec ou sans contact.

Avantageusement, grâce au procédé selon l'invention, seule une entité d'authentification légitime peut reconnaître l'identité de l'entité cliente cherchant à s'authentifier. L'identité de l'entité cliente A cherchant à s'authentifier n'est connue que de l'entité d'authentification B et n'est jamais révélée au cours de l'authentification. De plus, l'entité cliente A ne sait pas sous quel nom elle est identifiée par l'entité d'authentification. L'entité qui s'authentifie n'a en fait aucune identité statique qui pourrait être révélée. D'autre part, en faisant en sorte qu'une entité refuse de s'authentifier en présence d'une question qui lui a déjà été soumise, un tiers malveillant est incapable de distinguer des entités. Au vue de deux authentifications successives, il n'est pas possible de dire si ce sont

deux entités distinctes ou la même entité qui se sont authentifiées. L'anonymat est donc complet.

REVENDICATIONS

1. Procédé d'authentification d'au moins une entité cliente (A) par une entité d'authentification (B), ladite entité d'authentification (B) comprenant un ensemble de clés secrètes (K_{Ai}), chacune étant associée à une entité cliente (Ai) susceptible d'être identifiée par ladite entité d'authentification, ledit procédé étant caractérisé en ce qu'il comprend les étapes suivantes consistant à :

a-transmettre une demande d'authentification anonyme (DemandeAuthentification) de la part de l'entité cliente (A) vers l'entité d'authentification (B) ;

b-envoyer de l'entité d'authentification (B) vers l'entité cliente (A), une valeur de compteur d'authentification (CB) correspondant à l'état courant d'un compteur (COMPTB) de l'entité d'authentification (B) ;

c-vérifier, côté entité cliente (A), que la valeur de compteur d'authentification (CB) reçue est strictement supérieure à une valeur de compteur (CA) mémorisée par l'entité cliente ;

d-calculer, côté entité cliente (A), une signature de compteur par application d'une fonction cryptographique (S) partagée par l'entité cliente et l'entité d'authentification, avec comme opérandes ladite valeur de

compteur d'authentification (CB) et une clé secrète (K_A) associée à l'entité cliente (A) ;

e-transmettre ladite signature ($S(K_A, CB)$) de compteur à l'entité d'authentification (B) ;

f-mettre à jour la valeur de compteur (CA) mémorisée par l'entité cliente (A) avec ladite valeur de compteur d'authentification (CB) ;

g-rechercher, côté entité d'authentification (B), au moins une entité cliente (Ai) susceptible d'être identifiée, pour laquelle la signature de compteur correspondante ($S(K_{Ai}, CB)$) pour ladite valeur de compteur d'authentification (CB) est cohérente avec la signature de compteur reçue ($S(K_A, CB)$) ;

h-faire croître le compteur d'authentification (COMPTB).

2. Procédé d'authentification selon la revendication 1, caractérisé en ce que les étapes b) à h) sont réitérées au moins une fois, de sorte à s'assurer que l'entité cliente identifiée est identique à chaque itération.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que l'étape de recherche consiste à :

i-calculer, pour chaque entité cliente (Ai) susceptible d'être identifiée, la signature de compteur correspondante ($S(K_{Ai}, CB)$) par application de la fonction cryptographique (S) avec comme opérandes la valeur de compteur d'authentification (CB) et la clé

secrète associée (K_{Ai}), de sorte à établir une liste de couples entité cliente susceptible d'être identifiée/signature de compteur correspondante (Ai, $S(K_{Ai}, CB)$), pour ladite valeur de compteur (CB) ;

j-vérifier la cohérence entre la signature de compteur reçue ($S(K_A, CB)$) et au moins une signature de compteur ($S(K_{Ai}, CB)$) de ladite liste.

4. Procédé d'authentification selon la revendication 3, caractérisé en ce que la liste des couples entité cliente susceptible d'être identifiée/signature de compteur correspondante (Ai, $S(K_{Ai}, CB)$) établie pour une valeur de compteur d'authentification (CB) donnée, est ordonnée, côté entité d'authentification, selon la valeur de ladite signature de compteur ($S(K_{Ai}, CB)$).

5. Procédé d'authentification selon la revendication 3 ou 4, caractérisé en ce qu'en cas de cohérence entre la signature de compteur reçue (S(KA, CB)) et la signature de compteur ($S(K_{Ai}, CB)$) d'une pluralité de couples, les étapes b) à h) sont réitérées jusqu'à obtention d'un couple unique pour lequel la signature de compteur correspond à la signature de compteur reçue.

6. Procédé d'authentification selon la revendication 5, caractérisé en ce que, lors de la répétition de l'étape i), la signature de compteur ($S(K_{Ai}, CB)$) est calculée uniquement pour les entités clientes (Ai) correspondant à ladite pluralité de couples déterminée à l'itération précédente.

7. Procédé d'authentification selon l'une quelconque des revendications 3 à 5, caractérisé en ce qu'il consiste à mettre en œuvre l'étape i) de manière anticipée par rapport à une demande d'authentification issue d'une entité cliente (A) à l'étape a), ladite étape i) anticipée consistant à pré-établir, côté entité d'authentification (B), pour au moins une valeur de compteur d'authentification (CB) à venir, la liste des couples entité cliente susceptible d'être identifiée/signature de compteur correspondante (Ai, $S(K_{Ai}, CB)$) pour chacune desdites valeurs de compteur d'authentification à venir, et à mémoriser lesdites listes pré-établies côté entité d'authentification (B), tout envoi de l'entité d'authentification (B) vers l'entité cliente (A) d'une valeur de compteur d'authentification (CB), correspondant à l'envoi d'une valeur de compteur d'authentification (CB) pour laquelle une liste des couples entité cliente susceptible d'être identifiée/signature de compteur correspondante (Ai, $S(K_{Ai}, CB)$) a déjà été pré-établie.

8. Procédé d'authentification selon l'une quelconque des revendications précédentes, caractérisé en ce que l'étape h) consiste à faire croître le compteur d'authentification (COMPTB) d'un pas fixe.

9. Procédé d'authentification selon l'une quelconque des revendications 1 à 7, caractérisé en ce que l'étape h) consiste à faire croître le compteur d'authentification (COMPTB) d'un pas aléatoire.

10. Procédé d'authentification selon l'une quelconque des revendications 1 à 8, caractérisé en ce que, en réponse à une demande d'authentification, l'étape b) consiste à envoyer, côté entité d'authentification (B), en plus de la valeur de compteur d'authentification (CB), une valeur aléatoire associée à ladite valeur de compteur (CB), ladite valeur aléatoire étant différente pour chacune des valeurs de compteur d'authentification envoyée, chaque étape de signature de compteur mise en œuvre au cours dudit procédé étant remplacée par une étape de signature du couple valeur de compteur d'authentification/valeur aléatoire associée, consistant en l'application de la fonction cryptographique (S) comprenant en plus comme opérande ladite valeur aléatoire associée.

11. Procédé d'authentification selon l'une quelconque des revendications précédentes, caractérisé en ce que l'étape c) consiste en outre à vérifier que la différence entre la valeur de compteur d'authentification (CB) reçue et la valeur de compteur (CA) mémorisée par l'entité cliente est inférieure ou égale à une valeur prédéterminée.

12. Procédé d'authentification selon l'une quelconque des revendications 1 à 10, caractérisé en ce que, l'étape c) n'étant pas vérifiée, les étapes intermédiaires suivantes sont mises en œuvre consistant à :

-envoyer de l'entité cliente (A) vers l'entité d'authentification (B), la valeur de compteur (CA) mémorisée par l'entité cliente ;

-envoyer de l'entité d'authentification (B) vers l'entité cliente (A), une valeur de compteur d'authentification temporaire supérieure à ladite valeur de compteur (CA) mémorisée par l'entité cliente, puis à :

-mettre en oeuvre les étapes d) à g) sur la base de la valeur de compteur d'authentification temporaire et, en cas de succès de l'authentification de ladite entité cliente,

-mettre à jour la valeur de compteur d'authentification (CB) correspondant à l'état courant du compteur (COMPTB) de l'entité d'authentification (B) avec la valeur de compteur d'authentification temporaire et mettre en œuvre l'étape h).

13. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'étape e) consiste à transmettre en outre à l'entité d'authentification (B) la valeur de compteur d'authentification (CB).

14. Procédé d'authentification selon l'une quelconque des revendications précédentes, caractérisé en ce que la valeur de compteur d'authentification (CB) est codée sur au moins 128 bits.

15. Carte à puce, caractérisé en ce qu'elle comprend un circuit intégré et des moyens de mémorisation d'une clé secrète (K_A) et de mise en œuvre du procédé selon l'une quelconque des revendications 1 à 14.

16. Carte à puce selon la revendication 15, caractérisé en ce qu'il s'agit d'une carte à puce sans contact.

17. Entité d'authentification (B) d'au moins une entité cliente (A), caractérisé en ce qu'elle comprend un lecteur de carte à puce doté de moyens pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 14.

18. Entité d'authentification selon la revendication 17, caractérisé en ce qu'elle comprend un lecteur de carte à puce sans contact.

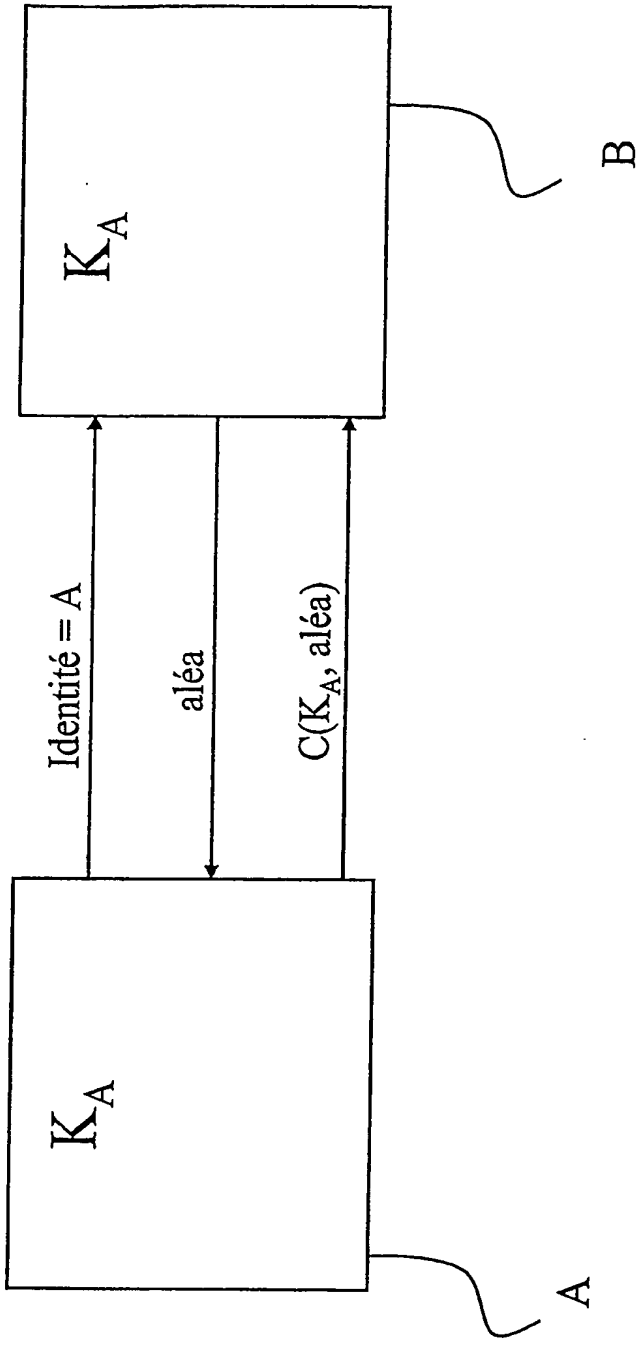

Fig.1
(art antérieur)

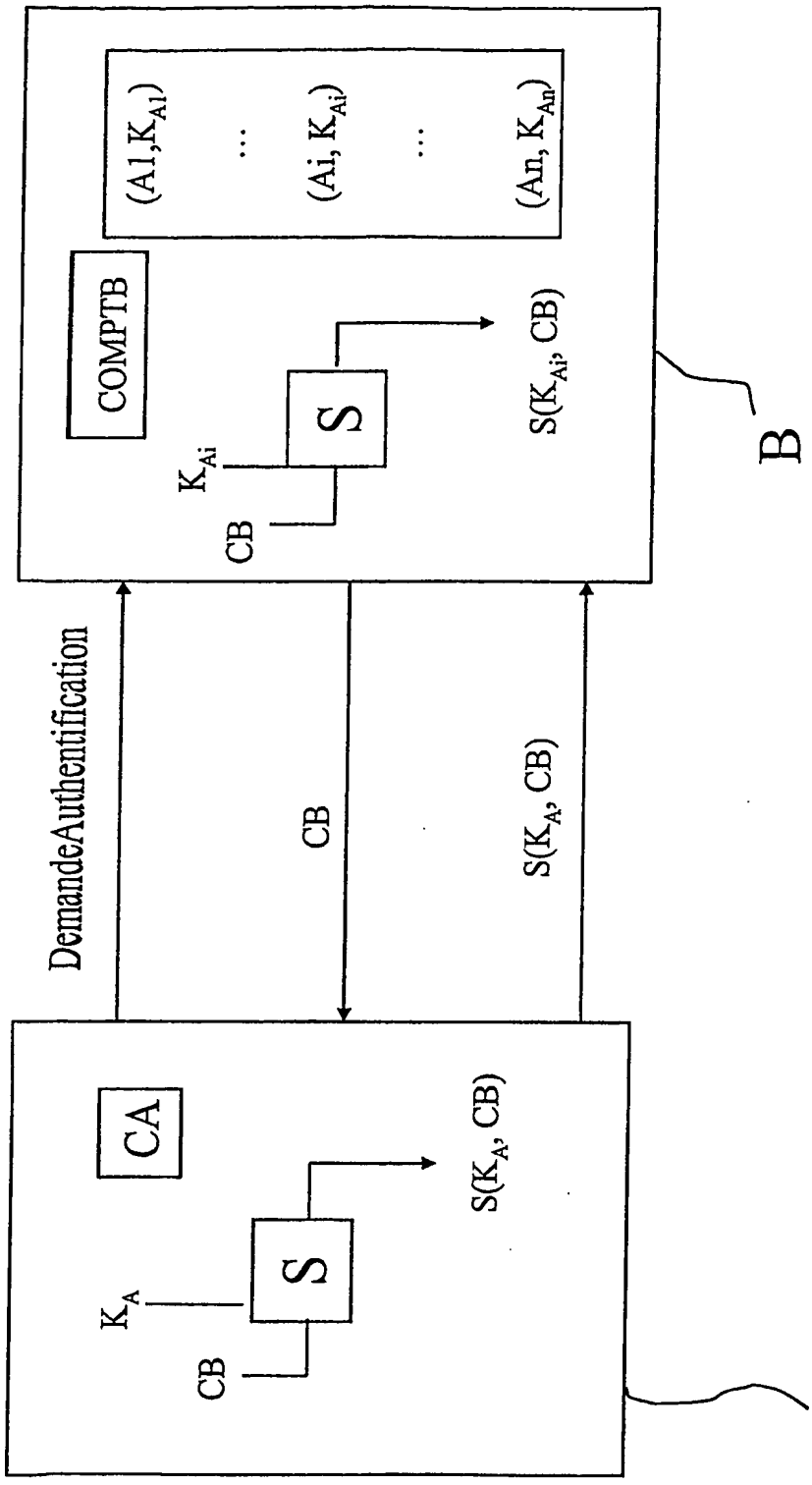
DemandeAuthentification
CB
S(K_A, CB)
CA
S
K_A
CB
S(K_A, CB)
A
COMPTB
(A1,K_A1)
(Ai, K_Ai)
(An, K_An)
S
K_Ai
CB
S(K_Ai, CB)
B

Fig.2